MICROPROCESSOR WITH PROTECTION CIRCUITS TO SECURE THE ACCESS TO ITS REGISTERS

Field of the Invention

The present invention relates to microprocessors, and, more particularly, to a microprocessor provided with protection circuits designed to secure access to the registers of the microprocessor.

Background of the Invention

A register in a microprocessor is generally selected as follows. The control unit of the microprocessor generates the address of the register to be selected and applies it to the address bus of the microprocessor. This address is transmitted to an address decoder which then selects the register relating to the address by activating the selection input of this register. The register can then be read or its contents can be modified. This register is, for example, an address register or an instruction register.

It sometimes happens that the contents of the registers of the microprocessor are accidentally modified when a mistake is made, or when there is a malfunction of the system in the microprocessor, especially during the initialization of the microprocessor.

Summary of the Invention

An object of the invention is to provide a microprocessor that ensures secured access to its registers.

According to the invention, it is planned, after each initialization of the microprocessor, to prevent any access to the registers of this microprocessor and to permit access to a register only if a password proper to this register has been presented at the data bus of the microprocessor during the first operation of selection of this register.

The microprocessor comprises an address bus, a data bus, a plurality of read accessible and write accessible registers, and an address decoder to select the registers as a function of the address present in the address bus.

The microprocessor furthermore comprises a plurality of protection circuits each associated with a register of the microprocessor to secure the access to the register. The protection circuits automatically block selection of the registers after each resetting of the microprocessor. The releasing of a protection circuit associated with a microprocessor register is done by the successive sending, on the data bus, of N passwords proper to the register during N first operations for the selection of the register with $N \geq 1$. The selection of the register is effective only for the subsequent operations for the selection of the register up to the following resetting of the microprocessor.

As needed, the protection circuit may block the selection of the associated register during operations of read access and write access to this register, or only during write access operations. During the N first operations for the selection of the associated register, each protection circuit compares the N data elements present in the data bus with the N passwords proper to the associated register. Each

protection circuit gets released for the subsequent operations of selection of the register up to the next resetting of the microprocessor if the N data elements correspond to the N passwords.

In one embodiment, only one password (N=1) is planned per register. The protection circuit then comprises a comparator circuit for the comparison, during the first operation of selection of the associated register, of the data element present in the data bus with the password proper to the register and for the delivery of an output signal representing the result of the comparison. First means hold the output signal in the protection circuit until the following resetting of the microprocessor. Second means permit the selection of the register for the subsequent selection operations of the register if the output signal indicates that the data present in the data bus of the microprocessor during the first operation of selection of the register corresponds to the password associated with the register.

Brief Description of the Drawings

Other features and advantages of the invention shall appear from the following detailed description made with reference to the appended drawings, of which:

FIG. 1 shows a first embodiment of a protection circuit according to the present invention to secure read access and write access to a register;

FIG. 2 shows a second embodiment of a protection circuit according to the present invention to secure write access to a register;

FIG. 3 shows a variation of the present invention by combining two protection circuits jointly securing access to two registers; and

FIG. 4 shows a third embodiment of a protection circuit according to the present invention to secure read and write access to a register.

Detailed Description of the Preferred Embodiments

The registers referred to hereinafter in the description comprise a selection input, a read/write input to which a read/write signal R/W- is applied and a data input/output connected to the data bus of the microprocessor. To implement the invention, a microprocessor, a portion of which is shown in FIG. 1, is provided with a protection circuit 1 to secure access to a register 3.

This protection circuit is interposed between the output of an address decoder 2 responsible for selecting the register 3 and the selection input of the register 3. The output of the decoder delivers a selection signal CS. According to the invention, one protection circuit per register is provided.

According to the invention, the protection circuit 1 is designed to automatically block the transmission of the selection signal CS after each resetting of the microprocessor. The protection circuit 1 is then released by the sending of a password proper to the register 3 on the data bus of the microprocessor during the first operation to select the register 3. The sending of a password on the data bus and the operation of selecting the register 3 are implemented, for example, during a cycle for writing the password in the register 3.

The first selection operation is used to release the protection circuit 1. The selection of the register 3 is effective only for the subsequent operations of selection of the register, up to the following resetting of the microprocessor. In the embodiment shown in FIG. 1, the protection circuit 1 blocks the selection of the register 3 during the

operations of read and write access to the register 3 after each resetting. According to one embodiment shown in FIG. 2, the protection circuit blocks the selection of the register 3 only during operations of write access to the register 3.

Referring to FIG. 1, the protection circuit essentially has a comparator circuit CP1 for the comparison, during the first operation for the selection of the register 3, of the data present on the data bus of the microprocessor with the password proper to the register 3. The comparator circuit CP1 delivers an output signal representing the result of the signal. The protection circuit also holds the output signal in the protection circuit up to the following resetting of the microprocessor. Finally, the protection circuit permits selection of the register for the subsequent operations for selecting the register if the output signal indicates that the data element present on the data bus of the register during the first operation for the selection of the register corresponds to the password associated with the register 3.

The comparator circuit CP1 has a selection input E1 connected to the output of the address decoder. This selection input E1 is responsible for selecting the register 3. The comparator CP1 comprises a data input E2 to receive the data present on the data bus and an output S delivering a value representing the result of the comparison between the data element on the data bus and the password associated with the register 3.

At its output S, it delivers a logic 1 if the two data elements are equal. Otherwise, it delivers a logic 0. The structure of a circuit of this kind is well known to those skilled in the art. The password associated with the register 3 may be either stored permanently in the comparator circuit CP1 or given by an external peripheral device (not shown).

The result of a logic 1 or 0 of this comparison is held in the protection circuit 1 up to the following resetting of the microprocessor by two D type flip-flop circuits, B1 and B2, each having a clock input CK, a signal input D, a resetting input RST and a signal output Q.

The clock input CK and the signal input D of the flip-flop circuit B1 respectively receive the selection signal CS and a logic 1. The signal input D is, for example, connected to a power supply source of the microprocessor. The signal output Q of this flip-flop circuit is connected to the clock input CK of the flip-flop circuit B2. The signal input D of the flip-flop circuit B2 is connected to the output S of the comparator circuit CP1. A resetting signal RESET is applied to the inputs RST of the flip-flop circuits B1 and B2 at each resetting of the microprocessor.

During the first operation for the selection of the register 3, the selection of the register 3 is effective only to prevent the password present on the data bus during this operation from being written in the register 3. Hence, in order that the selection of the register 3 may be permitted only from the second selection operation of the register 3 onwards, the Q output of the flip-flop circuit B2 is connected through a delay circuit RT1 to a first input of a two-input AND logic gate P1. The second input of the gate P1 is connected to the output of the address decoder 2, which is responsible for selecting the register 3. The output of the gate P1 is connected to the selection input of the register 3. The delay circuit RT1 is preferably a shift register synchronized with the selection signal CS.

The protection circuit works as follows. At each resetting of the microprocessor, the flip-flop circuits B1 and B2 are reset. During the first operation for the selection of the register 3, the

protection circuit 1 compares the data element present at the data output of the microprocessor with the password associated with the register 3. During this operation, the Q output of the flip-flop circuit B1 goes to a logic 1 and, on the resultant leading edge of the signal coming from this output, the Q output of the flip-flop circuit B2 delivers the result of the comparison. This result is then applied to the first input of the gate P1 with a delay to prevent the data element present on the data bus from being written in the register 3 during this first operation.

If the delay circuit RT1 is a shift register synchronized with the signal CS, the result of the comparison is applied to the first input of the gate P1 only starting with the second operation for the selection of the register 3. The password associated with the register 3 is preferably a data element not usually planned in the program of the microprocessor. This prevents the protection circuit from being accidentally released.

In a second embodiment shown in FIG. 2, the protection circuit is designed to secure only the write access of the register 3. The read access of the register 3 is never blocked. The releasing of the protection circuit, however, must be done during the first operation for the selection of the register as in the protection circuit of FIG. 1.

Referring to FIG. 2, the protection circuit 1 is complemented by a second two-input AND logic gate P2 and one two-input OR logic gate. The gate P2 has a first input connected to the output of the decoder 2 responsible for selecting the register 3 and a second input to which the read/write signal R/W- is applied. The outputs of the gates P1 and P2 are each connected to an input of the OR gate, and the output of the OR gate is connected to the selection input of the

register 3. Thus, the register 3 can be read at any time even if the protection circuit 1 is off.

In the case of an 8-bit microprocessor, there is a probability of 1/256 ($256 = 2^8$) that the data present on the data bus during the first register 3 selection operation caused by a malfunctioning of the system will be the password associated with the register 3. To reduce this probability, it is proposed, as a variation, to combine the protection circuits of several registers with each other. This embodiment is shown in FIG. 3.

In the example of FIG. 3, the protection circuits of two registers are combined to secure their access. In this example, the address decoder is responsible for selecting registers of the microprocessor, especially two registers 3 and 4. The elements B1, B2, CP1 and RT1 of the protection circuit 1 of FIG. 1 are combined in a block 5. A two-input AND logic gate P3 is interposed between the output of the block 5 and the first input of the gate P1. The output of the block 5 corresponds to the output of the delay circuit RT1. The output of the decoder 2 responsible for selecting the register 3 is connected to the input of the block 5 and to the second input of the gate P1.

A block 6, identical to the block 5, and an AND logic gate P4 form the protection circuit of the register 4 as described in FIG. 1. The comparator circuit of the block 6 is responsible for comparing the data element present on the data bus with a password associated with the register 4, distinct from the one associated with the register 3. The output of the block 6 is connected to a second input of the gate P3. The output of the decoder 2 responsible for selecting the register 4 is connected to the input of the block 6 and to the second input of the gate P4.

To obtain access to the registers 3 and 4, the operation for the releasing of the protection

circuit of FIG. 3 includes obtaining a write access to each register by applying the corresponding password to the data bus. These two write access operations must be performed during the first selection of the register 3 and during the first selection of the register 4. The register 3 can be selected before or after the register 4.

To further reduce this probability, a third embodiment of the protection circuit 1 is illustrated in FIG. 4. Access to the register 3 is secured by two passwords. These two passwords have to be placed on the data bus in a given order. For implementation of this protection circuit, the protection circuit of FIG. 1 is supplemented by two additional cascade-connected D type flip-flop circuits, B3 and B4, a second comparator circuit CP2 and a second delay circuit RT2. The clock input CK of the flip-flop circuit B3 is connected to the Q output of the flip-flop circuit B2 by a second delay circuit RT2. A logic 1 is applied to the D input of the flip-flop circuit B2, and its Q output is connected to the clock input CK of the flip-flop circuit B4.

The data input E2 of the comparator circuit CP2 is connected to the data bus, and its selection input E1 is connected to the output of the address decoder responsible for selecting the register 3. The S output of the comparator CP2 is connected to the D input of the flip-flop circuit B4, and the Q output of the flip-flop circuit B4 is connected to the delay circuit RT1. The two delay circuits are synchronized on the selection signal CS. The comparators CP1 and CP2 have the task, respectively, during the first and second operations for selecting the register 3, of comparing the data element present on the data bus with the first password and second password of the register 3.

To release this protection circuit, it is necessary not only to give the two passwords associated with the register 3 on the data bus, but to give them in the right order. The security of the access to the registers of the microprocessor is thereby improved. It is possible to further improve the security of the system by increasing the number of passwords associated with each register.